IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:	) Date: November 1, 2004
William Berson, et al.	) Attorney Docket No.: E-621
Serial No.: 08/886,516	) Customer No.: 00919
Filed: July 1, 1997	) Group Art Unit: 2137
Confirmation No.: 8901	) Examiner: Matthew Smithers

Title: METHOD OF PREVENTING COUNTERFEITING OF ARTICLES OF MANUFACTURE

TRANSMITTAL OF APPEAL BRIEF (PATENT APPLICATION 37 CFR 1.192)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Transmitted herewith in **triplicate** is the **APPEAL BRIEF** in the above-identified patent application with respect to the Notice of Appeal filed on September 3, 2004.

Pursuant to 37 CFR 1.17(c), the fee for filing the Appeal Brief is $340.00

Please charge Deposit Account No. **16-1885** in the amount of $340.00 to cover the above fee.

The Commissioner is hereby authorized to charge any additional fees which may be required to Deposit Account No. **16-1885**.

A duplicate copy of this transmittal is enclosed for use in charging the Deposit Account.

Respectfully submitted,

Ronald Reichman
Reg. No. 26,796
Attorney of Record
Telephone (203) 924-3854

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on November 1, 2004
Date of Deposit

Elizabeth P. Czarnecki
Name of Rep.

Elizabeth P. Czarnecki
Signature

November 1, 2004
Date

AF/2137

PATENT IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:	) Attorney Docket No.: E-621
William Berson, et al	) Group Art Unit: 2137
Serial No.: 08/886,516	) Examiner: Matthew Smithers
Filed: July 1, 1997	) Date: November 1, 2004

Customer No.: 00919

Title: **METHOD OF PREVENTING COUNTERFEITING OF ARTICLES OF MANUFACTURE**

APPELLANT'S BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This brief is in furtherance of the Notice of Appeal filed in this application on September 3, 2004.

This brief is transmitted in triplicate.

11/04/2004 RMEBRAHT 00000057 161885 08886516
01 FC:1402 340.00 DA

TABLE OF CONTENTS

This brief contains these items under the following headings and in the order set forth below:

I. REAL PARTY IN INTEREST

Pitney Bowes Inc. is the real party in interest by way of assignment from the Appellant.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A.) Claims 1-3 and 5-7 are in the application.

B.) Claims 1-3 and 5-7 are rejected.

C.) Claims 1-3 and 5-7 are on appeal.

IV. STATUS OF AMENDMENTS

An amendment subsequent to the June 7, 2004, Final Rejection was filed on July 23, 2004. This Amendment was not entered.

V. SUMMARY OF INVENTION

A. BACKGROUND

Counterfeiting and forgery of goods are well known problems. Manufacturers of luxury goods such as watches, luggage, perfume, etc. must constantly deal with counterfeiters who produce cheap imitations. Even inexpensive goods such as T-shirts can acquire considerable cachet, and associated high markup, by being marked with the image of a famous cartoon character, or other valuable, proprietary logo.

While the counterfeiting of consumer goods or other articles of manufacture presents a problem which is probably comparable to problems associated with the counterfeiting of documents which represent value (e.g., currency), until recently no comparable efforts have been made to combat this problem. While there is a long history of techniques such as elaborate engraving and use of special paper stocks to prevent counterfeiting of currency, in general, similar efforts have not been used even for the most expensive luxury goods.

An approach, which has been used to combat counterfeiting of documents, is the use of encryption. One method is encrypting information extracted from a document and imprinting the document with the encrypted information in order to verify the information contained in the document. Similarly with another method a document is scanned to produce a digital signal which is compressed, encrypted, and coded as a two dimensional bar code, which is incorporated into a label which is affixed to the document.

While these and other similar methods have been useful for their intended purpose, that purpose has been limited to the verification of the information content of a

document. In general, those who use such techniques either are not concerned that the information be duplicated so long as it is not altered, or, as with currency, are willing to rely on other techniques to detect duplication. Since much of the value of the sort of articles of manufacture, which are likely to be counterfeited, inheres in the fact that each particular item is essentially indistinguishable from other items of the same type, there has been, to Appellant's best knowledge, no previous attempt to use encryption techniques to verify the source of articles of manufacture.

B. APPELLANT'S CLAIMED INVENTION

1. Claim 1 relates to verifying the source of an article of manufacture, and for controlling the production of the article of manufacture by a licensee. More particularly, claim 1 relates to controlling a supply of labels from a licensor to the licensee to monitor the production of the article of manufacture; preparing a label by the licensee, the label having an unreproduceable pattern and information relating to the article; and encrypting at least a portion of the information by the licensor relating to the article.

Appellant's invention is a method for verifying the source of an article of manufacture. A label having information relating to the article is prepared and digitally signed or otherwise encrypted to authenticate the information. The label and a tangible representation of the digital signature or other encrypted information are then securely associated with the article. The information relating to the article can include verifying information such as an expiration date, unique identification of the article, identification of an authorized provider of the article or a description of the article to protect against

unauthorized use of duplicate labels. The label can also include an unreproduceable pattern such as a pattern of magnetic fibers randomly distributed and embedded in the label and a digitally signed description of the pattern. The unrreproducible pattern could alternatively be produced by spattering ink or paint drops.

Appellants claimed invention is shown in Fig. 1 and described in line 14 of page 4 to line 13 of page 6 of Appellants' Patent Application. A copy Fig.1 appears below.

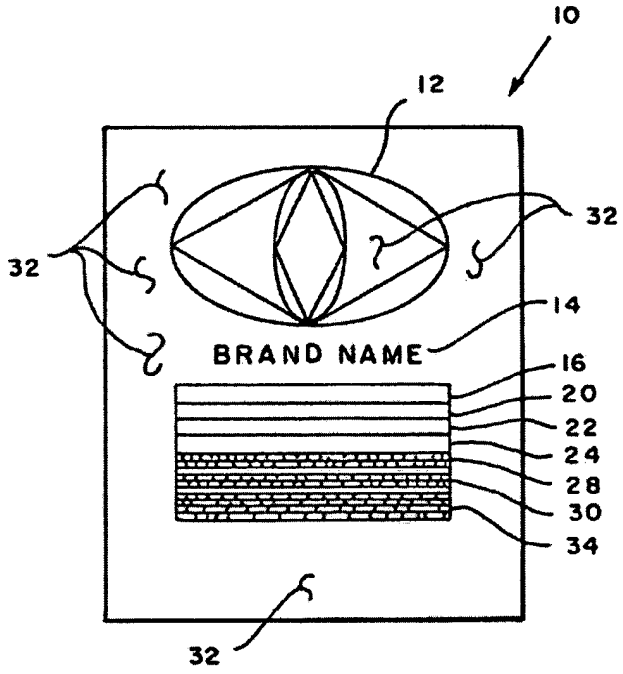


Fig. 1 shows label 10 which can be used in accordance with the subject invention to verify the source of an article of manufacture. Label 10 can include conventional logo 12 and/or brand name 14, as well as any other information, which might normally be found on a product label. Additionally, in one embodiment of the subject invention, verifying information is included in field 16, 20, 22, and 24. These fields might contain, for example, a serial number uniquely identifying a particular article, a description of such article in terms of size, color, model, etc., the identity of an authorized provider or

re-seller of such an article, or an expiration date beyond which a sale would not be authorized. As will be described further below, such verifying information provides a degree of protection against the unauthorized use of duplicate labels since a particular label will have only limited usefulness in terms of the time, place, or articles with which it may be used.

All, or selected portions, of the information on label 10 is then replicated in a scannable form in field 28. Preferably, the information is replicated in the form of a two dimensional bar code such as is specified in the well-known PDF 417 standard. All, or selected parts, of the information on label 10 is then digitally signed in a conventional manner in field 30.

In accordance with the subject invention, a manufacturer or authorized provider of an article of manufacture prepares a label such as shown in Fig. 1 using an encryption key, which the manufacturer or other authorized provider keeps in secret. Label 10 is then securely associated with the article; typically by affixing it to the article so that it cannot be removed without destroying it.

Further, label 10 need not comprise a single element. For example, the information in field 28 and/or the digital signature in field 30 may be printed on an invoice or manifest which accompanies the article. As noted above, secure association of label 10 with an article of manufacture requires only that it be made sufficiently difficult or expensive in some manner so that it is likely that the cost of unauthorized re-use of label 10 will exceed any benefit.

While the use of verifying information as described above limits the ability of a counterfeiter to use duplicate labels, some articles of particularly great value may

require more nearly total protection. This is achieved in accordance with one embodiment of the subject invention by incorporation of an unreproduceable pattern in or on label 10. Such a pattern is shown as elements 32 in Fig. 1. Preferably elements 32 are magnetic fibers (claim 5) as are described in U.S. Patent No. 5,003,291; to: Strom-Olsen; issued: March 26, 1991 which is hereby incorporated by reference, which is incorporated in the stock on which label 10 is printed when the stock is manufactured. Since the fibers are randomly distributed through the stock as it is formed, the distribution pattern of such fibers in a particular label cannot be reproduced without extraordinary effort. When the label is produced, unreproduceable pattern 32 is scanned and a tangible representation, which is preferably a barcode representation, is incorporated in field 34 and digitally signed together with the information in field 28. A very high degree of confidence, of the authenticity of label 10,may then be achieved by scanning patterns 32 and comparing it to the description in field 34. Verification of the description in field 34 will then verify the authenticity of label 10.

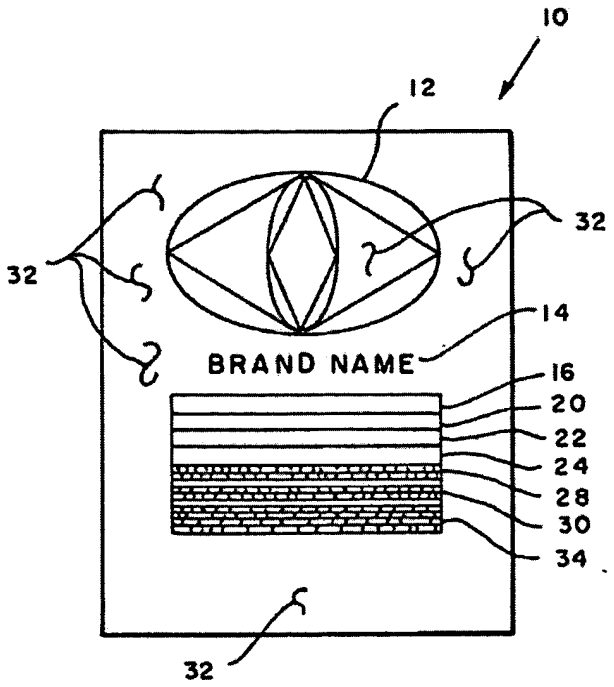
Methods for detecting the presence of magnetic fibers are known and are described in the above-referenced U.S. Patent No. 5,003,291 and a sufficiently precise description may be generated by scanning label 10 with a detector having a sufficiently small aperture.

The method of the subject invention may also be used to control the production of articles by licensees of trademarks or other intellectual property. The trademark licenser may control the supply of labels to the trademark licensee to control or monitor the number of articles produced. Alternatively, the licensee may label the articles as described above while the licenser controls the process of digitally signing the labels.

It should also be noted that stock having an unreproduceable pattern in combination with an encrypted or digitally signed description of that pattern can be used to produce valuable documents such as currency, or security tapes used to provide evidence of tampering.

Digital signing is a well-known technique for showing that information has not been changed, wherein a portion of the information selected by a "hash function" is encrypted to provide a "digital signature". By again applying the "hash function" to the information and comparing the result to the decrypted signature the information may be verified. However, other protocols wherein all or part of the particular information is encrypted in order to assure its authenticity are known and such techniques are within the contemplation of the sub-convention.

2. Claim 3 depends on claim 2 which depends on claim 1, wherein the verifying information includes information consisting of: an expiration date, a unique identification of said article of manufacture, an identification of a provider of said article of manufacture, or information describing said article of manufacture.



Additionally, in one embodiment of the subject invention shown in Fig. 1 and described in line 17 –23 of page 3, verifying information is included in field 16, 20, 22, and 24. These fields might contain, for example, a serial number uniquely identifying a particular article, a description of such article in terms of size, color, model, etc., the identity of an authorized provider or re-seller of such an article, or an expiration date beyond which a sale would not be authorized.

3. Claim 6 depends on claim 1. In claim 6, the encrypted information is encrypted with a first private key of a first public/private key pair and a corresponding first public key is available to parties who wish to validate the source of said article.

In another preferred embodiment of the subject invention, described in lines 21 – 31 of Appellant's specification the information on label 10 (Fig. 1) is digitally signed using the private key of a public/private key pair. (Public/private key encryption is a

known encryption technique where one key of a key pair is used to encrypt data and the other to decrypt the data and the private key cannot be determined from knowledge of the data and the public key.) Thus, the public key may be made widely available while the private key is kept in secret so that articles of manufacture may be readily verified in accordance with the subject invention but can only be so labeled by a manufacturer or authorized provider, having knowledge of the private key.

4. **Claim 7 depends on claim 6. In claim 7, a trusted third party provides a party producing the label with the first private key and with an encryption of the first public key by a second private key kept secret by the trusted third party, the producing party including the encryption of the first public key with the label and the trusted third party providing a corresponding second public key to parties who wish to verify the source of the article; whereby the parties can recover the first public key from the label so that articles from a large number of different sources can be verified without the need to maintain a corresponding database of public keys.**

One disadvantage of such a system as described in lines 1 –13 of Appellant's specification is that where a large a number of parties are providing articles to a single party for verification. The verifying party is then faced with the problem of maintaining a database of public keys for each of the providing parties. This problem can be overcome in accordance with another embodiment of the subject invention by means of a "nested key" system, wherein a trusted third party delivers distinct private, encryption keys to each of the providing parties together with a corresponding decryption key which has been encrypted with the third party's private, encryption key. The providing

parties then digitally sign label 10 as described above and incorporate the encrypted decryption key on label 10. Any party wishing to verify label 10 need only have knowledge of the trusted third party's public, decryption key to recover the decryption key needed to verify digitally signed label 10.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether or not claims 1, 2 and 5 are patentable under 35 U.S.C. 103(a) over U.S. Patent 5,365,586 granted to Indeck et al. and further in view of U. S. Patent No. 5,940,504 granted to Griswold.

B. Whether or not claim 3 is patentable under 35 U.S.C. 103(a) over U.S. Patent 5,365,586 granted to Indeck et al. and further in view of U. S. Patent No. 5,940,504 granted to Griswold.

C. Whether or not claim 6 is patentable under 35 U.S.C. 103(a) over U.S. Patent 5,365,586 granted to Indeck et al. and further in view of U. S. Patent No. 5,940,504 granted to Griswold.

D. Whether or not claim 7 is patentable under 35 U.S.C. 103(a) over U.S. Patent 5,365,586 granted to Indeck et al. and further in view of U. S. Patent No. 5,940,504 granted to Griswold and U.S. Patent No. 5,638,446 granted to Rubin.

VII. ARGUMENTS

A. Claims 1 and 5 have been rejected by the Examiner under 35 U.S.C. 103(a) over U.S. Patent 5,365,586 granted to Indeck et al. and further in view of U. S. Patent No. 5,940,504 granted to Griswold.

Indeck discloses the following in the abstract:

> "A method and apparatus is disclosed for determining the remanent noise in a magnetic medium by DC saturation of a region thereof and measurement of the remaining DC magnetization. A conventional magnetic recording transducer may be used to determine the remanent noise. Upon determination, the remanent noise may then be digitized and recorded on the same magnetic medium to thereby "fingerprint" the magnetic medium. This "fingerprint" may then be later used to verify and authenticate the magnetic medium as being an original. In such manner, any magnetic medium, or any object having an associated magnetic medium, may be "fingerprinted" including credit cards, computer programs, compact discs, videotapes, cassette tapes, etc."

Indeck discloses the following in lines 23-28 of column 6, which the Examiner is of the opinion discloses step (a) of claim 1:

> "As shown in **FIG. 3**, the magnetic "fingerprint" at a specified region **40** of a thin film magnetic medium or tape **42**, shown representationally in **FIG.** 3 as a thin film tape, may be recorded at a second position **44** on said thin film magnetic medium or tape **42** in a digitized, machine readable bar code **46** or the like."

Indeck discloses the following in lines 30-40 of column 4, which the Examiner is of the opinion discloses step (b) of claim 1:

> "This remanent noise, which is an analog signal, may then be digitized and recorded, in the medium itself or elsewhere, in machine readable format using a trap door function. Thusly, the magnetic medium has become "labeled" with its fingerprint. Verification or authentication of that magnetic medium is simply achieved by reversing this process except that the digitally

> recorded fingerprint must be decrypted using the publicly known key. Should the measured remnant noise match the remanent noise as recorded, the magnetic medium is authenticated."

Indeck discloses the following in lines 35-41 of column 2, which the Examiner is of the opinion discloses step (c) of claim 1:

> "The light intensity function determined by the unique random pattern of paper fibers along the line then forms the fingerprint of the particular piece of paper. This fingerprint is then digitized and encrypted by the secret encryption function. The encrypted fingerprint is then separately printed onto the paper in digital form such as a bar code."

Indeck discloses the following in lines 5-14 of column 3, which the Examiner is of the opinion discloses step (d) of claim 1:

> "The density variations are randomly created as the magnetic medium is applied, which affords a unique document as these density variations are fixed and repeatable to identify the document. A second magnetic stripe is also applied to the document, but this magnetic stripe is comprised of a medium that is tightly specified and highly controlled in accordance with well known standards in the recording art to be part of a magnetic read/write system."

Indeck relates to a method and apparatus for fingerprinting magnetic media. The fingerprinting is accomplished by determining the remanent noise in a magnetic medium by DC saturation of a region thereof and measurement of the remaining DC magnetization. Indeed, Indeck is directed to generating a fingerprint at a specific region of a thick film magnetic medium or tape.

Griswold discloses the following in his abstract:

> "A license management system and method for recording the use of a licensed product, and for controlling its use in accordance with the terms of the license. A licensed product

> invokes a license check monitor at regular time intervals. The monitor generates request datagrams which identify the licensee and the product and sends the request datagrams over a communications facility to a license control system. The license control system maintains a record of the received datagrams, and compares the received datagrams to data stored in its licensee database. Consequently, the license control system transmits reply datagrams with either a denial or an approval message to the monitor. The monitor terminates further use of the product if it receives a denial message. The monitor generates its own denial message if its request datagrams are unanswered after a predetermined interval of time. The datagrams are counted at the control system to provide billing information."

Griswold discloses the following in lines 19-37 of column 5:

> "As shown in **FIG. 1**, a licensed product **1** is located at a licensee's site. Product **1** may include a data portion **1B** and a functional portion **1A** such as computer software product or any other kind of information product used to control use of data portion **1B**. If data portion **1B** is CD-ROM database information, functional portion **1A** should enable the licensee to search indexes and display text. If data portion **1B** is video information, functional portion **1A** should control the display of the video information. For audio information, functional portion **1A** should play the audio information. If data portion **1B** is an electronic book, functional portion **1A** should display and turn pages. The above examples sow some of the ways functional portion **1A** can control data portion **1B**; however, they are hardly exhaustive.
>
> By including in product **1** both information and software which controls the information, product **1** is an executable product. Non-software information in product **1** is preferably encrypted so that it cannot be easily extracted from the product."

Griswold discloses a license management system and method, which can ensure that a licensed product is used only on machines under which it is licensed. Thus, Griswold does not disclose or anticipate a method for verifying the source of an article

of manufacture and for controlling the production of the article of manufacture by a licensee.

Neither Indeck nor Griswold, taken separately or together, discloses or anticipates a method for verifying the source of an article of manufacture and for controlling the production of the article of manufacture by a licensee that includes steps a, b and d of claim 1, namely, a) controlling a supply of labels from a licensor to the licensee to monitor the production of the article of manufacture; b) preparing a label by the licensee, the label having an unreproduceable pattern and information relating to the article; and d) encrypting at least a portion of the information by the licensor relating to the article.

Notwithstanding the foregoing, in rejecting a claim under 35 U.S.C. §103, the Examiner is charged with the initial burden for providing a factual basis to support the obviousness conclusion. ***In re Warner,*** 379 F.2d 1011, 154 USPQ 173 (CCPA 1967*);* ***in re Lunsford,*** 375 F.2d 385, 148 USPQ 721 (CCPA 1966); ***in re Freed***, 425 F.2d 785, 165 USPQ 570 (CCPA 1970). The Examiner is also required to explain how and why one having ordinary skill in the art would have been led to modify an applied reference and/or combine applied references to arrive at the claimed invention. ***In re Ochiai***, 37 USPQ2d 1127 (Fed. Cir. 1995); **in re Deuel**, *51 F.3d 1552, 34 USPQ 1210 (Fed. Cir. 1995);* ***in re Fritch***, 972 F.2d 1260, 23 USPQ 1780 (Fed. Cir. 1992); ***Uniroyal, Inc. v. Rudkin-Wiley Corp.***, 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988). In establishing the requisite motivation, it has been consistently held that both the suggestion and reasonable expectation of success must stem from the prior art itself, as a whole. ***In re Ochiai***, supra; **in re Vaeck**, *947 F.2d 488, 20 USPQ2d 1438*

(Fed. Cir. 1991); ***in re Fine***, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); ***in re Dow Chemical Co.***, 837 F.2d 469, 5 USPQ2d 1529 (Fed. Cir. 1988).

B. Claim 3 has been rejected by the Examiner under 35 U.S.C. 103(a) over U.S. Patent 5,365,586 granted to Indeck et al. and further in view of U. S. Patent No. 5,940,504 granted to Griswold.

The Examiner indicated in page 3 of the June 7, 2004, Final Rejection that: " Regarding claim 3, Indeck as modified verifying information consisting of information about the article of manufacture (see Indeck col. 4, lines 24 – 40)"

Indeck discloses the following in col. 4, lines 7 – 40:

> "To reproduce this distribution, intentionally or not, is practically impossible since this would entail a precise manipulation of the orientation of innumerable particles at the submicrometer level. Thus, the orientation of a large set of particles on a specific portion of a recording surface can uniquely identify that medium. In experiments, the inventors have found that the remanent noise from a length of between about 30 micrometers and 4300 micrometers provides enough data to "fingerprint" a magnetic medium.
>
> In essence, the present invention is elegantly simple and adapted for implementation by conventional recording heads as are commonly found and used in virtually every read or read/write device presently utilized by the public at large. Such examples include credit card readers, magneto-optic disc players, cassette players, VCRs and personal computers. In its simplest implementation, a conventional recording head need merely DC saturate a specified portion of a magnetic medium, and then "read" or "play back" the remanent noise which remains. Alternatively, the fingerprint can be obtained from the region between two recorded magnetic transitions. This remanent noise, which is an analog signal, may then be digitized and recorded, in the medium itself or elsewhere, in machine readable format using a trap door function. Thusly, the magnetic medium has become "labeled" with its fingerprint. Verification or authentication of that magnetic medium is simply achieved by reversing this process except that the digitally

> recorded fingerprint must be decrypted using the publicly known key. Should the measured remnant noise match the remanent noise as recorded, the magnetic medium is authenticated."

In addition to the arguments made in above Section A, Indeck does not disclose or anticipate, in the environment of claim 1, verifying information that includes information consisting of: an expiration date, a unique identification of said article of manufacture, an identification of a provider of said article of manufacture, or information describing said article of manufacture.

C. Claim 6 has been rejected by the Examiner under 35 U.S.C. 103(a) over U.S. Patent 5,365,586 granted to Indeck et al. and further in view of U. S. Patent No. 5,940,504 granted to Griswold.

The Examiner indicated in page 3 of the June 7, 2004, Final Rejection that: "Regarding claim 6, Indeck as modified is met by the description at column 4, lines 35 - 38)"

Indeck discloses the following in col. 4, lines 35 - 38:

> "Verification or authentication of that magnetic medium is simply achieved by reversing the process except that the digitally recorded fingerprint must be decrypted using the publicly known key. Should the measured remmant noise match the remanent noise as recorded, the magnetic medium is authenticated."

In addition to the arguments made in above Section A, Indeck does not disclose or anticipate the encrypted information of claim 1 in the environment of claim 1, being encrypted with a first private key of a first public/private key pair and a corresponding first public key that is available to parties who wish to validate the source of said article.

E. Claim 7 has been rejected by the Examiner under 35 U.S.C. 103(a) over U.S. Patent 5,365,586 granted to Indeck et al. and further in view of U. S. Patent No. 5,940,504 granted to Griswold and U.S. Patent No. 5,638,446 granted to Rubin.

The Examiner indicated in page 4 of the June 7, 2004, Final Rejection that:

> "Indeck as modified discloses verification using the publicly known key at column 4, lines 35-38. However, the instant claims provide for signing of the public key by a trusted third party. The patent to Rubin teaches a secure distribution of electronic files. The files are signed by the source of the files (the authors) and the public key of the authors is signed with the secret key of a trusted third party, see Figure 2, blocks 30, 32 and 34. It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to sign the public key of the source as taught in Rubin in order to provide a public key of a source with the certification of a trusted third party."

Rubin discloses the following in col. 5, lines 54 - 67:

> "T then uses A's public key to verify that the message came from A (i.e. that the hash of the message was encrypted using A's private key) and that the date is current, step 30. T then generates an electronic certificate 32 containing the following information: i) the identity of T, ii) the name of the hash function used, iii) author's name, iv) authors address, v) author's organization, vi) author's email address, vii) file name, viii) file location, ix) cryptographic hash of the file as sent by A, and x) date.
>
> After generating the certificate, T signs it with its private key, step 34. T can send the certificate to A or store it in a

publicly accessible location and notify A as to where it is stored, or both."

Rubin uses a hash function, which is then digitally signed.

In addition to the arguments made in above Section A, Rubin does not disclose or anticipate the encrypted information of claim 1 in the environment of claims 1 and 6, where a trusted third party provides a party producing the label with the first private key and with an encryption of the first public key by a second private key kept secret by the trusted third party, the producing party including the encryption of the first public key with the label and the trusted third party providing a corresponding second public key to parties who wish to verify the source of the article; whereby the parties can recover the first public key from the label so that articles from a large number of different sources can be verified without the need to maintain a corresponding database of public keys.

Thus, Appellant's claimed encryption scheme is more restrictive than Rubin's. Since, Appellant's are encrypting which hides the first public key from parties who do not have access to the second public key and Rubin is digitally signing which places the first public key in the clear.

VIII. PRAYER FOR RELIEF

Appellants respectfully submit that appealed claims 1 - 3 and 5 - 7 in this application are patentable. It is requested that the Board of Appeal overrule the Examiner and direct allowance of the rejected claims.

Respectfully submitted,

Ronald Reichman
Reg. No. 26,796
Attorney of Record
Telephone (203) 924-3854

PITNEY BOWES INC.
Intellectual Property and Technology Law Department
35 Waterview Drive, P.O. Box 3000
Shelton, CT 06484-8000

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on November 1, 2004
Date of Deposit

Elizabeth P. Czarnecki
Name of Rep.

Elizabeth P. Czarnecki
Signature

November 1, 2004
Date

IX. Claims Appendix A

1. A method for verifying the source of an article of manufacture, and for controlling the production of the article of manufacture by a licensee, the method comprising the steps of:

a) controlling a supply of labels from a licensor to the licensee to monitor the production of the article of manufacture;

b) preparing a label by the licensee, the label having an unreproduceable pattern and information relating to the article;

c) processing the unreproduceable pattern and including the processed unreproduceable pattern with the information relating to the article;

d) encrypting at least a portion of the information by the licensor relating to the article; and

e) securely associating the article, the label, and a tangible representation of the encrypted information.

2. A method described in Claim 1 wherein said information included on said label includes verifying information for protecting against unauthorized use of duplicate labels.

3. A method as described in Claim 2 wherein said verifying information includes information consisting of: an expiration date, a unique identification of said

article of manufacture, an identification of a provider of said article of manufacture, or information describing said article of manufacture.

5. A method as described in Claim 1 wherein said unreproduceable pattern is formed from magnetic fibers embedded in said label.

6. A method as described in Claim 1 wherein said encrypted information is encrypted with a first private key of a first public/private key pair and a corresponding first public key is available to parties who wish to validate the source of said article.

7. A method as described in Claim 6 wherein a trusted third party provides a party producing said label with said first private key and with an encryption of said first public key by a second private key kept secret by said trusted third party, said producing party including said encryption of said first public key with said label and said trusted third party providing a corresponding second public key to parties who wish to verify the source of said article; whereby said parties can recover said first public key from said label so that articles from a large number of different sources can be verified without the need to maintain a corresponding database of public keys.